IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.:	09/694,416
Filing Date:	October 20, 2000
Applicant:	Thomas Collins et al.
Group Art Unit:	2131
Examiner:	James Seal
Title:	PUBLIC KEY CRYPTOGRAPHIC APPARATUS AND METHOD
Attorney Docket:	6215-000124/US/RED

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

October 14, 2003

AMENDMENT AFTER FINAL

Sir:

In response to the Office Action mailed April 11, 2003, the due date having been extended three (3) month to October 11, 2003, the following amendments and remarks are respectfully submitted in connection with the above-identified application.

Amendments to the Claims begin on page two of this Amendment.

IN THE CLAIMS

1. (Previously Presented) A method for communications of a message cryptographically processed with RSA (Rivest, Shamir & Adleman) public key encryption, comprising the steps of:

developing k distinct random prime numbers $p_1, p_2,\ldots,p_k$, where k is an integer greater than 2;

providing a number e relatively prime to $(p_1 -1)\cdot(p_2 -1)\cdot\ldots\cdot(p_k -1)$;

providing a composite number n equaling the product $p_1\cdot p_2\cdot\ldots\cdot p_k$;

receiving a ciphertext word signal C which is formed by encoding a plaintext message word signal M to a ciphertext word signal C, where M corresponds to a number representative of the message and

$0\leq M\leq n-1$,

where C is a number representative of an encoded form of the plaintext message word signal M such that $C\equiv M^e \pmod n$, and where e is associated with an intended recipient of the cipherhext word signal C; and

deciphering the received ciphertext word signal C at the intended recipient having available to it the k distinct random prime number $p_1, p_2, \ldots p_k$.

2. (Previously Presented) The method according to claim 1, wherein the deciphering step includes

establishing a number, d, as a multiplicative inverse of e(mod(1cm($(p_1 -1), (p_2 -1), \ldots, (p_k -1)$))), and

decoding the ciphertext word signal C to the plaintext message word signal M where $M\equiv C^d \pmod n$.

3. (Previously Presented) A method for communications of a message signal M_i cryptographically processed with RSA public key encryption in a system having j terminals, each terminal being characterized by an encoding key $E_i =(e_i, n_i)$ and a decoding key $D_i=(d_i, n_i)$, where i=1, 2, ... , j, and the meassage signal M_i corresponds to a number representative of a message-to-be-received from the i^{th} terminal, the method comprising the steps of:

establishing n_i where n_i is a composite number of the form

$n_i = p_{i,1} \cdot p_{i,2} \cdot , \ldots , \cdot p_{i,k}$

where k is an integer greater than 2,

$p_{i,1}$, $p_{i,2}$, ..., $p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to lcm($p_{i,1}$ -1, $p_{i,2}$-1, ... $p_{i,k}$ -1), and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

e_i(mod(lcm(($p_{i,1}$ -1), ($p_{i,2}$ -1), ..., ($p_{i,k}$ -1))));

receiving by a recipient terminal (i = y) from a sender terminal (i = x, x ≠ y) a ciphertext signal C_X formed by encoding a digital message word signal M_x, wherein the encoding includes

transforming said message word signal M_x to one or more message block word signals M_x", each block word signal M_x" corresponding to a number representative of a portion of said message word signal M_x in the range $0 \leq M_X" \leq n_y - 1$, and

transforming each of said message block word signals M_X" to a ciphertext word signal C_X that corresponds to a number representative of an encoded form of said message block word signal M_X" where $C_X \equiv M_X"^{ey} \pmod{n_y}$; and

deciphering the received ciphertext word signal C_x at the recipient terminal having available to it the k distinct random prime numbers $p_{y,1}$, $p_{y,2}$, ..., $p_{y,k}$ for establishing its d_y.

4. (Currently Amended) A system for communications of a message cryptographically processed with an RSA public key encryption comprising:

a communication channel for transmitting a ciphertext word signal C;

encoding means coupled to said channel and adapted for transforming a transmit message word signal M to the ciphertext word signal C using a composite number, n, where n is a product of the form

$n = p_1 \, p_2 \cdot \ldots \cdot p_k$

k is an integer greater than 2, and

p_1, p_2, ... p_k are distinct random prime numbers, where the transmit message word signal M corresponds to a number representative of the message and

$0 \leq M \leq n-1$

where the ciphertext word signal C corresponds to a number representative of an encoded form of said message through a relationship of the form

$C \equiv\_ M^e \pmod{n}$, and

where e is a number relatively prime to [[lcm(p1 - 1, p2 -1, ..., pk -1)]] lcm(p_1 - 1, p_2 -1, ..., p_k -1); and

decoding means coupled to said channel and adapted for receiving the ciphertext word signal C from said channel and, having available to it the k distinct random prime number p_1, p_2, ... p_k, for transforming the ciphertext word signal C to a receive message word signal M' where M' corresponds to a number representative of a decoded form of the ciphertext word signal C through a relationship of the form $M' \equiv\_ C^d \pmod{n}$

where d is selected from the group consisting of a class of numbers equivalent to a multiplicative inverse of

e(mod(1cm((p_1 -1), (p_2 -1), ..., (pk -1)))).

5. (Previously Presented) A system for communications of a message crytographically processed with an RSA public key encryption, the system having a plurality of terminals coupled by a communications channel, comprising:

a first terminal of the plurality of terminals characterized by an encoding key

$E_A = (e_A, n_A)$ and a decoding key $D_A = (d_A, n_A)$,

where n_A is a composite number of the form

$n_A = p_{A,1} \cdot p_{A,2} \cdot \ldots \cdot p_{A,k}$

where

k is an integer greater than 2,

$p_{A,1}$, $p_{A,2}$, ..., $p_{A,k}$ are distinct random prime numbers,

e_A is relatively prime to

lcm($p_{A,1}$-1, $p_{A,2}$-1, ..., $p_{A,k}$-1), and

d_A is selected from the group consisting of the class of numbers equivalent to a multicative inverse of

e_A (mod(lcm(($p_{A,1}$ -1), ($p_{A,2}$-1), ..., ($p_{A,k}$ -1)))); and

a second terminal of the plurality of terminals having blocking means for transforming a first message, which is to be transmitted on said communications channel from

said second terminal to said first terminal, into one or more transmit message word signals M_B, where each M_B corresponds to a number representative of said first message in the range of $0 \leq M_B \leq n_A-1$,

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_B to a ciphertext word signal C_B that corresponds to a number representative of an encoded form of said first message through a relationship of the form

$C_B \equiv M_B^{\ eA} \pmod{n_A}$,

said first terminal having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_B form said channel and, having available to it the k distinct

random prime numbers $p_{A,1}$, $p_{A,2}$, ... $p_{A,k}$, for transforming each of said ciphertext word signals C_B to a receive message word signal M'_B, and

means for transforming said receive message word signal M'_B to said first message, where M'_B corresponds to a number representative of a decoded form of C_B through a relationship of the form

$M'_B \equiv C_B^{dA} \pmod{n_A}$.

6. (Previously Presented) The system according to claim 5 wherein said second terminal is characterized by an encoding key $E_B=(e_B, n_B)$ and a decoding key $D_B=d_B, n_B)$, where

n_B is a composite number of the form

$n_B = p_{B,1}\, p_{B,2} \cdot \ldots \cdot p_{B,k}$

where k is an integer greater than 2,

$p_{B,1}$, $p_{B,2}$, ... $p_{B,k}$ are distinct random prime numbers,

e_B is relatively prime to

$\text{lcm}(p_{B,1}-1, p_{B,2}-1), \ldots, (p_{B,k}-1)$, and

d_B is selected from the group consisting of class of numbers equivalent to a multiplicative inverse of

$e_B \pmod{\text{lcm}((p_{B,1}-1), (p_{B,2}-1), \ldots, (p_{B,k}-1))}$,

said first terminal further having

blocking means for transforming a second message, which is to be transmitted on said communications channel from said first terminal to said second terminal, to one or more transmit message word signals M_A, where each M_A corresponds to a number representative of said message in the range $0 \leq M_A \leq n_B-1$

encoding means coupled to said channel and adapted for transforming each transmit message word signal M_A to a ciphertext word signal C_A and for transmitting C_A on said channel, where C_A corresponds to a number representative of an encoded form of said second massage through a relationship of the form

$C_A \equiv M_A^{eB} \pmod{n_B}$

said second terminal further having

decoding means coupled to said channel and adapted for receiving each of said ciphertext word signals C_A from said channel and, having available to it the k distinct

random prime numbers $p_{B,1}$, $p_{B,2}$, ... $p_{B,k}$, for transforming each of said ciphertext word signals to a receive message word signal M'_A, and

means for transforming said receive message word signals M'_A to said second message, where M'_A corresponds to a number representative of a decoded form of C_A through a relationship of the form $M'_A \equiv C_A^{dB} \pmod{n_B}$.

7. Cancelled

8. Cancelled

9. (Previously Presented) A system for communications of message signals cryptographically processed with RSA public key encryption, comprising:

j terminals including first and second terminals, each of the j terminals being characterized by an encoding key $E_i=(e_i, n_i)$ and decoding key $D_i-(d_i, n_i)$, where i=1,2,...,j, each of the j terminals being adapted to transmit a particular one of the message signals where an i^{th} message signal M_i is transmitted from an i^{th} terminal, and

$o \leq M_i \leq n_i-1$,

n_i being a composite number of the form

$n_i=p_{i,1}\ p_{i,2} \ldots p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to

$\text{lcm}(p_{i,1}-1, p_{i,2}-1, \ldots p_{i,k}-1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_i(\text{mod}(\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots, (p_{i,k}-1))))$;

said first terminal including

means for encoding a digital message word signal M_1 to be transmitted from said first terminal (i=1) to said second terminal (i=2), said encoding means transforming said digital message word signal M_1 to a signed message word signal M_{1s} using a relationship of the form

$M_{1s} \equiv M_1^{\ d1} \ (\text{mod}\ n_1)$; and

means for transmitting said signed message word signal M_{1s} from said first terminal to said second terminal, wherein said second terminal includes

means for decoding said signed message word signal M_{1s} to said digital message word signal M_1.

10. (Previously Presented) The system of claim 9, wherein the means for decoding said signed message word signal M_{AS} includes means for transforming said signed message word signal M_{AS} using a relationship of the form

$M_1 \equiv M_{ls}^{\ e1} \ (\text{mod}\ n_1)$.

11. (Previously Presented) A communications system for transferring a message signal cryptographically processed with RSA public key encryption, the communications system comprising:

j communication stations including first and second stations, each of the j communication stations being characterized by an encoding key $E_i=(e_i,n_i)$ and a decoding key $D_i=(d_i, n_i)$, where i-1, 2, ..., j, each of the j communication stations being adapted to transmit a

particular one of the message signals where an i^{th} message signal M_i is received from an i^{th} communication station, and

$0 \leq M_i \leq n_i - 1$

n_i being a composite number of the form

$n_i = p_{i,1} \cdot p_{i,2} \cdot \ldots \cdot p_{i,k}$

where

k is an integer greater than 2,

$p_{i,1}, p_{i,2}, \ldots p_{i,k}$ are distinct random prime numbers,

e_i is relatively prime to lcm $(p_{i,1} - 1, p_{i,2} - 1, \ldots, p_{i,k} - 1)$, and

d_i is selected from the group consisting of the class of numbers equivalent to a multiplicative inverse of

$e_i \, (\text{mod}(\text{lcm}((p_{i,1}-1), (p_{i,2}-1), \ldots., (p_{i,k}-1))))$,

said first station including

means for encoding a digital message word signal M_1 to be transmitted from said first station (i=1) to said second station (i=2),

means for transforming said digital message word signal M_1 to one or more message block word signals M_1", each block word signal M_1" being a number representative of a portion of said message word signal M_1 in the range

$0 \leq M_1" \leq n_2 - 1$, and

means for transforming each of said message block word signals M_1" to a ciphertext word signal C1 using a relationship of the form $C_1 \equiv M"_1{}^{e2} \pmod{n_2}$; and

means for transmitting said ciphertext word signals C_1 from said first station to said second station, wherein said second station includes

means for deciphering said ciphertext word signals C_1 using $p_{2,1}, p_{2,2} \ldots p_{2,k}$ to produce said message word signal M_1.

12. (Previously Presented) The communications system of claim 11, wherein the deciphering means includes

means for decoding said ciphertext word signals C_1 to said message block word signals M_1" using a relationship of the form

$M"_1 \equiv C_1{}^{d2} \pmod{n_2}$, and

means for transforming said message block word signals M_1" to said message word signal M_1.

13. Cancelled

14. (Previously Presented) A method of communicating a message cryptographically processed with an RSA public key encryption, comprising the steps of:

selecting a public key portion e associated with a recipient intended for receiving the message;

developing k distinct random prime numbers, p_1, p_2, ... p_k, where $k \geq 3$, and checking that each of the k_i distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message formed by encoding a plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, where M represents the message, where $0 \leq M \leq n-1$ and where the sender knows n and the public key portion e but has no access to the k distinct random prime numbers, p_1, p_2, ... p_k; and

deciphering at the recipient the received ciphertext message data C to produce the message, the recipient having access to the k distinct random prime numbers, p_1, p_2, ... p_k.

15. (Previously Presented) The method according to claim 14, comprising the further step of:

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1}(\mathrm{mod}((p_1 -1)\cdot(p_2 -1)\cdots(p_k -1)))$,

wherein the deciphering step includes decoding the ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

16. (Previously Presented) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, p_1, p_2, ... p_k, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

receiving a ciphertext message data C representing an encoded form of a plaintext message data M; and

decoding the received ciphertext message data C to the plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$, the decoding performed by a recipient owning the private key portion d and having access to the k distinct random prime numbers, p_1, p_2, ... p_k.

17. (Previously Presented) The method according to claim 16, wherein the ciphertext message data C is formed by encoding the plaintext message data M to the ciphertext message data C using a relationship of the form $C \equiv M^e \pmod{n}$, wherein $0 \leq M \leq n-1$ and wherein n and the public key portion e are accessible to the sender although it has no access to the k distinct random prime numbers, p_1, p_2, ... p_k.

18. (Previously Presented) A method of communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, p_1, p_2, ... p_k, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e of the form $d \equiv e^{-1} (\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers;

encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$

receiving the signed message M_s; and

deciphering the signed message to produce the plaintext message data M.

19. (Previously Presented) The method of claim 18, wherein the deciphering step includes:

decoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

20. (Previously Presented) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

sending to a recipient a cryptographically processed message formed by assigning a number M to represent the message in plaintext message form, and

cryptographically transforming the assigned number M from the plaintext message form to a number C that represents the message in an encoded form, wherein the number C is a function of

the assigned number M,

a number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e having been obtained by the sender are associated with the recipient to which the message is intended; and

receiving the cryptographically processed message which is decipherable by the recipient based on

the number n,

another exponent d, and

the number C,

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers.

21. (Previously Presented) The method according to claim 20,

wherein the cryptographically transforming step includes using a relationship of the form $C \equiv M^e \pmod{n}$,

wherein the exponent d is established based on the at least three distinct random prime numbers, $p_1, p_2, \cdots p_k$, using a relationship of the form $d \equiv e^{-1} (\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$, and

wherein the cryptographically processed message is deciphered using a relationship of the form $M \equiv C^d \text{ (mod n)}$.

22. (Previously Presented) A method for communicating a message cryptographically processed with RSA public key encryption, comprising the steps of:

receiving from a sender a cryptographically processed message, in the form of a number C, which is decipherable by the recipient based on a number n, an exponent d, and the number C; and

deciphering the cryptographically processed message,

wherein a number M represents a plaintext form of the message, wherein the number C represents a cryptographically encoded form of the message and is a function of the number M,

the number n that is a composite number equaling the product of at least three distinct random prime numbers, wherein $0 \leq M \leq n-1$, and

an exponent e that is a number relatively prime to a lowest common multiplier of the at least three distinct random prime numbers,

wherein the number n and exponent e are associated with the recipient to which the message is intended, and

wherein the exponent d is a function of the exponent e and the at least three distinct random prime numbers.

23. (Previously Presented) The method according to claim 22,

wherein the number C is formed using a relationship of the form $C \equiv M^e \text{ (mod n)}$,

wherein the exponent d is established based on the at lest three distinct random prime numbers, $p_1, p_2, \ldots p_k$, using a relationship of the form $d \equiv e^{-1} (\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

and wherein the number M is obtained using a relationship of the form $M \equiv C^d \text{ (mod n)}$.

24. (Previously Presented) The method according to claim 21,

wherein p and q are a pair of prime numbers the product of which equals n,

wherein the deciphering the number C to derive the number M is divided into subtasks, one subtask for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q,

whereby for a given length of n it takes fewer computational cycles to perform the deciphering relative to the number of computational cycles for performing such deciphering if the pair of prime numbers p and q were instead.

25. (Previously Presented) The method according to claim 22,

wherein p and q are a pair of prime numbers the product of which equals n,

wherein the deciphering the number C to derive the number M is divided into subtasks, one subtask for each of the k distinct random prime numbers,

wherein k distinct random prime numbers are each smaller than p and q,

whereby for a give length of n it takes fewer computational cycles to perform the deciphering relative to the number of computational cycles for performing such deciphering if the pair of prime numbers p and q were used instead.

26. (Previously Presented) The method according to claim 20,

wherein p and q are a pair of prime numbers the product of which equals n, and wherein developing the at least three distinct random prime numbers and computing n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

27. (Previously Presented) The method according to claim 22,

wherein p and q are a pair of prime numbers the product of which equals n, and

wherein developing the at least three distinct random prime numbers and computing n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

28. (Previously Presented) The method according to claim 14,

wherein p and q are a pair of prime numbers the product of which equals n,

wherein the deciphering step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller that p and q,

whereby for a given length of n it takes fewer computational cycles to perform the deciphering step relative to the number of computational cycles for performing such deciphering step if the pair of prime numbers p and q were used instead.

29. (Previously Presented) The method according to claim 14,

wherein p and q are a pair of prime numbers the product of which equals n, and

wherein developing the k distinct random prime numbers and computing the composite number n are performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

30. (Previously Presented) The method according to claim 16,

wherein p and q are a pair of prime numbers the product of which equals n,

wherein the decoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q,

whereby for a given length of n it takes fewer computational cycles to perform the decoding step relative to the number of computational cycles for performing such decoding step if the pair of prime numbers p and q were used instead.

31. (Previously Presented) The method according to claim 16,

wherein p and q are a pair of prime numbers the product of which equals n, and

wherein developing the k distinct random prime number and computing the composite n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

32. (Previously Presented) The method according to claim 18,

wherein p and q are a pair of prime numbers the product of which equals n,

wherein the encoding step is divided into sub-steps, one sub-step for each of the k distinct random prime numbers,

wherein the k distinct random prime numbers are each smaller than p and q,

whereby for a given length of n it takes fewer computational cycles to perform the encoding step relative to the number of computational cycles for performing such encoding step if the pair of prime numbers p and q were used instead.

33. (Previously Presented) The method according to claim 18,

wherein p and q are a pair of prime numbers that product of which equals n, and

wherein developing the k distinct random prime numbers and computing the composite number n is performed, including for n that is more than 600 digits long, in less time than it takes to develop the pair of prime numbers p and q and compute that n.

34. (Previously Presented) The method according to claim 14, wherein a message cryptographically processed by the sender with two-rime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable with multi-prime (k>2) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, ... p_k.

35. (Currently Amended) The method according to claim 9, wherein the signed message word signal M_{1s}, formed from the digital message word signal M_1 being cryptographically processed at the first terminal with multi-prime (k>2) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, ... [[pk]] p_k, is decipherable at the second terminal with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.

36. (Previously Presented) The method according to claim 16, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable by the decoding with multi-prime (k>2) RSA public key encryption characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, ... p_k.

37. (Previously Presented) The method according to claim 18, wherein the signed message M_s, formed from the plaintext message data M being cryptographically processed at the sender with multi-prime (k>2) RSA public key encryption which is characterized by the composite number n being computed as the product of the k distinct random prime numbers, p_1, p_2, ... p_k, is decipherable by the decoding at the recipient with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q.

38. (Previously Presented) The method according to claim 20, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to at composite number computed as the product of 2 prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

39. (Previously Presented) The method according to claim 22, wherein a message cryptographically processed by the sender with two-prime RSA public key encryption characterized by n being equal to a composite number computed as the product of 2 prime numbers p and q, is decipherable at the recipient with multi-prime RSA public key encryption characterized by the composite number n being computed as the product of the at least three distinct random prime numbers.

40. (Previously Presented) A cryptography method for local storage of data by a private key owner,

comprising the steps of:

selecting a public key portion e;

developing k distinct random prime numbers, p_1, p_2, ... p_k, where $k \geq 3$, and checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to the public key portion e;

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

computing a composite number, n, as a product of the k distinct random prime numbers that are factors of n, where only the private key owner knows the factors of n; and

encoding plaintext data M to ciphertext data C for the local storage, using a relationship of the form $C \equiv M^e \pmod{n}$, wherein $0 \leq M \leq n-1$, whereby the ciphertext data C is decipherable only by the private key owner having available to it the factors of n.

41. (Previously Presented) The cryptography method in accordance with claim 40, further comprising the step of:

decoding the ciphertext data C from the local storage to the plaintext data M using a relationship of the form $M \equiv C^d \pmod{n}$.

42. (Previously Presented) A cryptographic communications system, comprising:

a plurality of stations;

a communications medium; and

a host system adapted to communicate with the plurality of stations via the communications medium sending a receiving messages cryptographically processed with an RSA public key encryption, the host system including

at least one cryptosystem configured for

developing k distinct random prime numbers, p_1, p_2, ..., p_k, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ... p_k-1, is relatively prime to a public key portion e that is associated with the host system,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship of the public key portion e in the form of $d \equiv e^{-1} (\mathrm{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$,

in response to an encoding request from the host system, encoding a plaintext message data M producing therefrom a ciphertext message data C to be communicated via the host system, the encoding using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$,

in response to a decoding request from the host system, decoding a ciphertext message data C' communicated via the host producing therefrom a plaintext message data M' using a relationship of the form $M' \equiv C'^d \pmod{n}$.

43. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem communicatively coupled to and receiving from the bus encoding and decoding requests, the cryptosystem being configured for

providing a public key portion e,

developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$,

checking that each of the k distinct random prime numbers minus 1, $p_1-1, p_2-1, \ldots p_k-1$, is relatively prime to the public key portion e,

computing a composite number, n, as a product of the k distinct random prime numbers,

establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} \pmod{((p_1-1)\cdot(p_2-1)\cdots(p_k-1))}$,

in response to an encoding request from the bus, encoding a plaintext form of a first message M to produce C, a ciphertext form of the first message, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$, and

in response to an decoding request from the host system, decoding C', a ciphertext form of a second message, to produce M', a plaintext form of the second message, using a relationship of the form $M' \equiv C'_d \pmod{n}$, the first and second messages beign distinct or one and the same.

44. (Previously Presented) The system of claim 42, wherein the at least one cryptosystem includes

a plurality of exponentiators configured to operate in parallel in developing respective subtask values corresponding to the message.

45. (Previously Presented) The system of claim 42, wherein the at least one cryptosystem includes

a processor,

a data-address bus,

a memory coupled to the processor via the data-address bus,

a data encryption standard (DES) unit coupled to the memory and the processor via the data-address bus,

a plurality of exponentiator elements coupled to the processor via the DES unit, the plurality of exponentiator elements being configured to operate in parallel in developing respective subtask values corresponding to the message.

46. (Previously Presented) The system of claim 45, wherein the memory and each of the plurality of exponentiator elements has its own DES unit that cryptographically processes message data received/returned from/to the processor.

47. (Previously Presented) The system of claim 45, wherein the memory is partitioned into address spaces addressable by the processor, including secure, insecure and exponentiator elements address spaces, and wherein the DES unit is configured to recognize the secure and exponentiator elements address spaces and to automatically encode message data therefrom before it is provided to the exponentiator elements, the DES unit being bypassed when the processor is accessing the insecure memory address spaces, the DES unit being further configures to decode encoded message data received from the memory before it is provided to the processor.

48. (Previously Presented) The system of claim 45, wherein the at least one cryptosystem meets FIPS (Federal Information Processing Standard) 140-1 level 3.

49. (Previously Presented) The system of claim 45, wherein the processor maintains in the memory the public key portion e and the composite number n with its factors $p_1, p_2, \ldots p_k$.

50. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to develop subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding request providing a plaintext message M to be encoded,

obtaining a public key that includes an exponent e and a modulus n, a representation of the modulus n existing in the memory in the form of its k distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$,

constructing subtasks, one subtask for each of the k factors, to be executed by the exponentiator elements for producing respective ones of the subtask values, $C_1, C_2, \ldots C_k$, and

forming a ciphertext message C from the subtask values $C_1, C_2, \ldots C_k$,

wherein the ciphertext message C is decipherable using a private key that includes the modulus n and an exponent d which is a function of e.

51. (Previously Presented) The system of claim 50 wherein each one of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{\ ei} \pmod{p_i}$, where $M_i \equiv M \pmod{p_i}$, and $e_i \equiv e \pmod{p_i - 1}$, and where i=1,2,...k.

52. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

a bus; and

a cryptosystem receiving from the system via the bus encoding and decoding requests, the cryptosystem including

a plurality of exponentiator elements configured to developed subtask values,

a memory, and

a processor configured for

receiving the encoding and decoding requests, each encoding/decoding request provided with a plaintext/ciphertext message M/C to be encoded/decoded and with or without a public/private key that includes an exponent e/d and a modulus n a representation of which exists in the memory in the form of its k distinct random prime number factors $p_1, p_2, \ldots p_k$, where $k \geq 3$,

obtaining the public/private key from the memory of the encoding/decoding request is provided without the public/private key,

constructing subtasks to be executed by the exponentiator elements for producing respective ones of the subtask values, $M_1, M_2, \ldots M_k, /C_a, C_2, \ldots C_k$, and

forming the ciphertext/plaintext message C/M from the subtask values $C_1, C_2, \ldots C_k/M_1, M_1, \ldots M_k$.

53. (Previously Presented) The system of claim 52 wherein when produced each of the subtasks $C_1, C_2, \ldots C_k$ is developed using a relationship of the form $C_i \equiv M_i^{ei} \pmod{p_i}$, where $C_i \equiv C \pmod{p_i}$, and $e_i \equiv e \pmod{p_i - 1}$, and where $i = 1, 2, \ldots k$.

54. (Previously Presented) The system of claim 52 wherein when produced each one of the subtasks $M_1, M_2, \ldots M_k$ is developed using a relationship of the form $M_i \equiv C_i^{di} \pmod{p_i}$, where $M_i \equiv M \pmod{p_i}$, and $d_i \equiv d \pmod{p_i - 1}$, and where $i = 1,2,\ldots k$.

55. (Previously Presented) The system of claim 54, wherein the private key exponent d relates to the public key exponent e via $d \equiv e^{-1} \pmod{((p_1-1)\cdot(p_2-1)\cdots(p_k-1))}$.

56. (Previously Presented) A system for communications of a message cryptographically processed with RSA public key encryption, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, p_1, p_2, ... p_k, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1,...p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion e in the form of $d \equiv e^{-1} (\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers;

means for receiving a ciphertext message data C; and

means for decoding the ciphertext message data C to a plaintext message data M using a relationship of the form $M \equiv C^d \pmod{n}$.

57. (Previously Presented) The system according to claim 56, further comprising:

means for encoding the plaintext message data M to the ciphertext message data C, using a relationship of the form $C \equiv M^e \pmod{n}$, where $0 \leq M \leq n-1$.

58. (Previously Presented) A system for communications of a message cryptographically processed with

RSA public key encryption, comprising:

means for selecting a public key portion e;

means for developing k distinct random prime numbers, $p_1, p_2, \ldots p_k$, where $k \geq 3$, and for checking that each of the k distinct random prime numbers minus 1, p_1-1, p_2-1, ...p_k-1, is relatively prime to the public key portion e;

means for establishing a private key portion d by a relationship to the public key portion of the form $d \equiv e^{-1} (\text{mod}((p_1-1)\cdot(p_2-1)\cdots(p_k-1)))$;

means for computing a composite number, n, as a product of the k distinct random prime numbers; and

means for encoding a plaintext message data M with the private key portion d to produce a signed message M_s using a relationship of the form $M_s \equiv M^d \pmod{n}$, where $0 \leq M \leq n-1$, the signed message M_s being decipherable using the public key portion e.

59. (Previously Presented) The system of claim 58 further comprising the step of:

means for encoding the signed message M_s with the public key portion e to produce the plaintext message data M using a relationship of the form $M \equiv M_s^e \pmod{n}$.

60. (Previously Presented) The system of claim 57, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modulus value equal to n independent of the k distinct prime numbers.

61. (Previously Presented) The system of claim 59, wherein the system can communicate the cryptographically processed message to another system that encodes/decodes data with RSA public key encryption using a modules value equal to n independent of the k distinct prime numbers.

REMARKS

This amendment is filed in response to the final office action mailed April 11, 2003.

I. STATUS OF THE CLAIMS

As of the date of this Amendment, claims 1-6 and 9-12, 14-61 remain pending. Claims 4 and 35 have been amended and claims 7 and 13 have been cancelled as a result of this response.

II. OBJECTION TO THE SPECIFICATION

A. New Matter

Sections 11-16 of the Office Action indicate that Applicants' previous amendment of September 16, 2002 has been objected to under 35 U.S.C. § 132 as having allegedly introduced new matter into the specification.

In Section 12, the Examiner objects to the replacement to the term "using" with the term "extending". Applicants assert that the conventional RSA scheme uses two primes, whereas the present invention uses three or more. In this context, Applicants believe that the present invention "extends" the number of primes from two to three or more. As a result, Applicants believe that the present invention "extends" the RSA scheme. Accordingly, reconsideration and withdrawal of the objection is respectfully requested.

In Section 13, the Examiner asserts that the change that "three or more random large, distinct primed numbers are developed and checked to ensure that each (p_i-1) is relatively prime to e" is new matter.

Applicants direct the Examiner's attention to originally filed independent claim 1, filed on January 16, 1997 which recites e is a number relatively prime to $(p_1-1) \cdot (p_2-1) \cdot \ldots (p_k-1)$.

Accordingly, Applicants respectfully submit that the change to column 5, lines 31-33, merely brings the specification into compliance with original claim 1. Further, Applicants respectfully submit that one of ordinary skill in the art would recognize that the equation recited at column 5, line 39 would not work if three or more random large distinct prime numbers were not relatively prime to e. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In Section 14, the Examiner asserts that the amendment to column 5, line 52, to add a digital signature, is not supported. However, Applicants have been unable to locate the addition of a "digital signature" in Applicants previous response. Clarification of this rejection is requested.

In Section 15, the Examiner asserts that the amendment to the specification to column 6, line 24 to change "$i \geq 2$" to "$2 \leq i \leq k$ where k is the number of primes in n" constitutes new matter.

Applicants respectfully submit that this change merely more accurately recites the teachings of the present invention. As set forth clearly throughout the specification, there are no prime numbers beyond p_k; accordingly, it makes absolutely no sense to indicate prime numbers greater than equal to 2, but unbounded by the number of prime numbers k. Accordingly, Applicants respectfully submit that this is not new matter, but merely a reflection of the upper bound of the number of k primes, which the change of which, Applicants believe more accurately represents the present invention. However, although less accurate, Applicants are willing to leave this portion of the specification as "$i \geq 2$".

In Section 16, with regard to column 6, line 65, the Examiner asserts that the change from "the decrypted message M can be obtained" to "the ciphertext C can be obtained" is new matter.

The Examiner further asserts that in the first version, summation is required, wherein the second version iteration is required.

In response to this objection, Applicants respectfully submit that there are at least two know solutions for the Chinese Remainder Theorem. The first, proposed by Gauss, is a summation technique, and therefore not recursive. The second, proposed by Garner, is a recursive technique. Applicants respectfully submit that the original patent describes Garner's technique beginning at column 6, line 1 and Gauss' technique, beginning at column 7, line 1. Since the present application supports both recursive and non-recursive solutions, Applicants assert that the Amendment to column 6, line 65 does not constitute new matter.

III. CLAIM OBJECTIONS

In Sections 21 and 22, the Examiner points out minor informalities in the previous amendments to claims 4 and 35. Applicants have amended claims 4 and 35 to correct these minor informalities.

IV. CLAIM REJECTIONS UNDER 35 U.S.C. § 112

A. 35 U.S.C. § 112, FIRST PARAGRAPH

In Section 24, claim 1 is rejected under 35 U.S.C. § 112, first paragraph but no specific rejection is set forth. Applicants assume this rejection is related to the objection to the specification under 35 U.S.C. § 132 and therefore traversed for the reasons set forth above.

In Sections 25 and 26, the Examiner asserts that claims 1-2, 18-19, 32-33, 37, 42-49, and 56-61 are rejected under 35 U.S.C. § 112, first paragraph, because the patent as originally filed does not disclose $k \geq 3$. Applicants respectfully submit that column 3, line 27-29 of the original

Collins et al. patent recite that it is an object of the present invention is to provide a system and method for utilizing "multiple (more than two) distinct prime number components to create n." Further, column 3, lines 40-41 of the original Collins et al. patent recite that "n is developed from three or more distinct prime numbers; i.e., $n = p_1 \cdot p_2 \cdot \ldots p_k$, where k is an integer greater than two." Finally, column 5, lines 66-67 recite an example assuming three distinct primes, p_1, p_2, and p_3. Accordingly, Applicants respectfully submit that an amendment reciting k is an integer greater than two is supported by multiple passages in the original Collins et al. patent.

In Sections 27-29, the Examiner asserts that claims 1-61 are rejected under 35 U.S.C. § 112, first paragraph, objecting to the term "random". The Examiner correctly points out that the term random is utilized in the original patent at column 5, line 31 and is therefore supported by the original patent. Applicants assert that this disclosure supports the claims as amended.

In Applicants previous Response, Applicants asserted that "the randomness and distinctness attributes of the k prime numbers will materially improve the security in any cryptographic system with RSA public key encryption".

With respect to this statement, the Examiner asserts that if this were the intent of the original patent, the original patent does not support this view. Applicants respectfully submit that the above statement is an advantage of the present invention. Advantages of the present invention need not be provided in the specification In re Chu, 36 U.S.P.Q.2d 1089 (Fed.Cir. 1995). Accordingly, Applicants respectfully submit that claims 1-61 are supported by the original specification, because random is provided in the original patent, and any purported advantage of the randomness need not be present in the original patent.

In Sections 30 and 31, the Examiner rejects claims 7 and 13 for failing to describe how the equation recited therein is carried out. Applicants direct the Examiner's attention to the cancellation of independent claims 7 and 13, which render this rejection moot.

B. 35 U.S.C. 112, SECOND PARAGRAPH

In Sections 32 and 33, the Examiner objects to the relationship in claims 7 and 13 as being used to mean an "RSA public encryption". Applicants direct the Examiner's attention to the cancellation of independent claims 7 and 13, which render this rejection moot.

In Section 34, the Examiner objects to amended claim 9, specifically the word "means" is not followed by a function. Applicants have reviewed claim 9 and are unsure of the Examiner's rejection, in particular, each means clause of claim 9 appears to recite a function.

VI. CLAIM REJECTION UNDER 35 U.S.C. § 103

A. SUMMARY OF CLAIM REJECTIONS

In sections 35-76 of the Office Action, claims 1-7, 9-61 are rejected under 35 U.S.C. § 103(a). In sections 36-65 of the Office Action, claims 1-7, 9-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 4,405,829 to Rivest et al., henceforth RSA, and further in view of Rivest et al. "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Communications of the ACM, 21(2) February 1978, henceforth Rivest and further in view of Knuth, The Art of Computer Programming Vol. 2, page 179.

In formulating the rejection of claims 1-7 and 9-61 in view of RSA, Rivest, and Knuth in paragraphs 35-39, the Examiner picks and chooses various portions of three publications to piece together the subject matter of the present claims. Applicants assert that it impermissible to use

the claimed invention as an instruction manual or template to piece together the teachings of the prior art so that the claimed invention is rendered obvious. It is established U.S. patent law that one cannot use hindsight reconstruction to pick and choose among isolated disclosures in the prior art to deprecate the claimed invention.

Obviousness can not be established by combining the teachings of the prior art to produce the claimed invention, absent a teaching or suggestions supporting the combination. Under § 103, the teachings of references can be combined only if there is some suggestion or incentive to do so. Applicants further respectfully submit that this tenant of U.S. patent law also applies to separate embodiments of the same patent or patent publication. Applicants respectfully submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of the RSA patent, the Rivest publication, and Knuth, in order to piece together the invention recited in the presently pending claims. Accordingly, Applicants respectfully submit that claims 1-7 and 9-61 are allowable for at least this reason.

In Sections 66-68, claims 7 and 13 are rejected in view of RSA and Rivest and further in view of Schwenk US 5,835,598. This rejection is moot in light of the cancellation of these claims.

In Sections 69-70, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 are rejected under 35 U.S.C. § 102(b) as being anticipated by Vanstone and Zuccherato, "Using four-prime RSA in which some bits are Specified", Electronic Letters, 30(25), 16 August 1994, henceforth Vanstone.

In paragraph 70, the Examiner asserts that "Vanstone selects random primes even though he makes bit assignments in an expanding product ...". Applicants respectfully submit that this statement is wholly unsupported by Vanstone. Vanstone makes absolutely no mention of

random prime numbers. Accordingly, Applicants respectfully submit that claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, and 60-61 are allowable for at least this reason.

In Sections 72-74, claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo (RSA Moduli Should Have 3 Prime Factors), and further in view of Rivest et al.

With respect to Nemo, Applicants respectfully assert that this publication was submitted by Applicants during prosecution of the original application with no date, since applicants were unable to ascertain the publication date of the Nemo paper. Nemo was printed on the front of U.S. Patent 5,848,159 with "No Date or Publication Given".

During the prosecution of the present application, the Examiner has adopted the publication date of Nemo as August 1996, relying on a footnote on page 1 which states "the original version of this article may be obtained from Scientific Bulgarian Magazine, August 1996". Applicants respectfully assert that the fact this paper was submitted by a pseudonym as "Captain Nemo" and alleges to have been published in a fictitious publication, namely "Scientific Bulgarian", casts sufficient doubt as the date of the publication to render it insufficient to be relied upon as prior art against the present application. As set forth in M.P.E.P. § 706.02(a), the Examiner must determine the issue or publication date of a reference of a proper comparison between the application and the reference dates can be made. Applicants respectfully assert that the fictitious author in a fictitious journal, namely "Scientific Bulgarian", cast doubt on the accuracy of August 1996 as a publication date. Until the Examiner is able to verify the publication date of the Nemo publication as qualifying as prior art against the present application under 35 U.S.C. § 102(a) or (b) Applicants respectfully submit that Nemo cannot be applied

against the present application. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In Section 75, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Itakura and Nakamura, A Public-Key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No. 71, October, and further in view of Rivest et al. This rejection, insofar as it pertains to the presently pending claims, is respectfully traversed for the following reasons.

Initially, Applicants respectfully submit that the scheme described in Itakura and Nakamura provides no security. Accordingly, the purpose of this publication is completely different from the purpose of the present invention.

The goal of the Itakura et al. scheme is to create signatures appropriate for use in a business hierarchy. An individual at a higher level has a different "r" from an individual at a lower level and the lower level employee should not be able to forge the higher rank signature. Accordingly, Applicants respectfully submit that Itakura et al. is irrelevant to the present invention. Additionally, in exemplary embodiments of the present invention, all the primes are part of the private key and the security relies on the primes not being known. As set forth above, in Itakura et al., the third prime "r" is public. Accordingly, Applicants respectfully submit that claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are allowable over Itakura et al. for at least this reason. Additionally, an advantage of exemplary embodiments of the present invention is to obtain the security of a large "n" by increasing the number factors, instead of the size of the factors. In contrast, Itakura et al. stated in the first paragraph of 3.3 that increasing the length of the third prime "r" increases the length of "n" without increasing the security of the system.

For the reasons set forth above, Applicants respectfully assert that claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are allowable over Itakura et al. in view of Rivest et al.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 1-6, 8-12, and 13-61 in connection with the present application is earnestly solicited.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant(s) hereby petition(s) for a three (3) month extension of time for filing a reply to the outstanding Office Action. The fee for extension fee of $950.00 is being paid under the Notice of Appeal concurrently filed herewith.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-2025 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/cah